CLAIMS

1. A system for delivering institutional data to a customer, comprising:

an institutional server, wherein the institutional server includes a system for separately serving a first database containing private data and a second database containing public data;

a service provider, wherein the service provider includes a system for receiving an encrypted version of the private data and an unencrypted version of the public data; and

a client, wherein the client includes a system for displaying a merged version of the private and public data.

2. The system of claim 1, wherein the client includes a mechanism for decrypting the encrypted private data.

3. The system of claim 1, further comprising a system for making the customer anonymous to the service provider.

4. The system of claim 3, wherein the system for making the customer anonymous to the service provider includes a mechanism for determining a service level available to the customer.

5. The system of claim 1, wherein the service provider includes a system for analyzing the use of the public data by the customer without knowing an identity of the customer.

6. The system of claim 1, wherein the merged version of the private and public data is downloaded to the client by the service provider.

7. The system of claim 1, wherein the private and public data are downloaded to the client by the institutional server and service provider, respectively.

8. The system of claim 1, wherein the encrypted version of the private data is encrypted using a public key infrastructure protocol.

9. The system of claim 1, wherein the client includes an interface that can be customized into a first window for viewing the public data and a second window for viewing the private data.

10. A method of preserving privacy between a customer and an institution in a computer network environment, comprising the steps of:

separating data associated with the institution into a first database of private data and a second database of public data;

storing an encrypted copy of the private data and an unencrypted copy of the public data with an intermediary service provider;

providing to the customer a security system that allows the customer to decrypt the encrypted data and remain anonymous to the intermediary service provider;

merging the encrypted copy of the private data and the unencrypted copy of the public data; and

providing an interface that allows the customer to view the merged data.

11. The method of claim 10, wherein the security system includes a public key infrastructure protocol.

12. The method of claim 10, comprising the further step of customizing the interface to include a first window for viewing the public data and a second window for viewing the private data.

13. The method of claim 10, wherein the public data includes data available externally to the institution.

14. A method of preserving privacy between a customer and an institution in a computer network environment, comprising the steps of:

separating data associated with the institution into a first database of encrypted private data and a second database of public data;

loading an unencrypted copy of the public data to a service provider;

loading to a client the encrypted private data from the institution and the unencrypted copy of the public data from the service provider;

providing to the customer a security mechanism that allows the customer to decrypt the encrypted data and remain anonymous to the service provider; and

providing an interface that allows the customer to view the encrypted copy of the private data and the unencrypted copy of the public data.

15. The method of claim 14, wherein the security mechanism includes a public key infrastructure protocol.

16. The method of claim 14, comprising the further step of customizing the interface to include a first window for viewing the public data and a second window for viewing the private data.

17. The method of claim 14, wherein the public data includes data available externally to the institution.

18. A program product stored on a recordable medium that when executed, preserves privacy between a customer and an institution in a computer network environment, comprising:

a system for separating data associated with the institution into a first database of encrypted data and a second database of unencrypted data;

a system for providing a copy of the second database of unencrypted data to an intermediary service provider;

an interface that allows the customer to view the first database of encrypted data and the copy of the second database of unencrypted data provided to the intermediary service provider; and

a security system that allows the customer to decrypt the encrypted data and remain anonymous to the intermediary service provider.

19. The program product of claim 18, further comprising:

a system for providing a copy of the first database of unencrypted data to the intermediary service provider.